CLAIMS

I claim:

1. A communications architecture for a security network containing at least a first and a second base unit and a first transponder, wherein

5   -   The said first transponder communicates to at least the first base unit using low power wireless communications, and

       -      The said second base unit communicates with the said first base unit using high power wireless communications.

2. The communications architecture in claim 1 wherein the said low power wireless

10   communications operates at a different frequency band than the said high power wireless communications.

3. The communications architecture in claim 1 wherein the said low power wireless communications operates under a different FCC rule section than the said high power wireless communications.

15 4. The communications architecture in claim 1 wherein the said low power wireless communications is transmitted at average power levels under 10 milliwatts and the said high power wireless communications is transmitted at average power levels above 10 milliwatts.

5. The communications architecture in claim 1 wherein the said low power wireless

20   communications operates within a first fixed frequency range and the said high power communications never operates within the first fixed frequency range.

6. The communications architecture in claim 1 wherein the said first transponder can receive wireless communications from the said first base unit.

7. The communications architecture in claim 6 wherein the said first transponder can change

25   parameters of subsequent transmitted low power wireless communications based upon data received in the wireless communications from the said first base unit.

8. The communications architecture in claim 1 wherein when the said first base unit can receive a first communications from the first transponder and send a copy of the said first communications to the said second base unit.

9. The communications architecture in claim 1 wherein the communications sent from the said first transponder contains identifying information that identifies the first transponder.

10. The communications architecture in claim 1 wherein the communications sent from the said first transponder contains identifying information that identifies the security network in which the first transponder is enrolled.

11. The communications architecture in claim 1 wherein at least part of the communications sent from the said first transponder has been encrypted using an encryption key.

12. The communications architecture in claim 1 wherein the communications sent from the said first transponder to the said first base unit is received by the said second base unit.

13. The communications architecture in claim 9 wherein the said first base unit contains first data used by the said first base unit to determine whether to send a copy of the communications sent from the said first transponder to the said second base unit.

14. The communications architecture in claim 13 wherein the said first data includes identifying information about the said first transponder.

15. The communications architecture in claim 11 wherein the said first base unit contains an encryption key than enables the said first base unit to interpret the said communications sent by the said first transponder to the said first base unit.

16. The communications architecture in claim 1 wherein the first base unit is in the physical form of a cordless phone handset.

17. The communications architecture in claim 1 wherein the second base unit is in the physical form of a cordless phone handset.

18. The communications architecture in claim 1 wherein the second base unit is in the physical form of a cordless phone base station.

19. The communications architecture in claim 1 wherein the first base unit is powered by a battery.

20. The communications architecture in claim 12 wherein the said second base unit sends a copy of the said communications sent from the said first transponder to the said first base unit using high power wireless communications.